

WHAT IS CLAIMED IS:

1. A method of providing distributed web server authentication of a valid user requesting access to a web server, said method comprising:

receiving a request to connect the valid user to a web server;
creating a user password cookie using a shared secret key; and
transmitting the user password cookie in response to the request to connect.

2. The method of claim 1, wherein creating a user password cookie using a shared secret key, comprises:

reading a user credential cookie;
requesting a user identification (ID) and password;
receiving the user ID and password; and
validating the valid user's identity.

3. The method of claim 2, wherein validating the valid user's identity, comprises:
authenticating the user ID and password with the user credential cookie using a local authenticating mechanism.

4. The method of claim 3, wherein the local authenticating mechanism is an operating system.

5. The method of claim 2, wherein creating a user password cookie using the shared secret key, further comprises:
combining at least the user ID and password with a time stamp; and
encrypting the combined at least user ID, password and time stamp using the shared secret key.

6. The method of claim 1, wherein creating a user password cookie using a shared secret key, comprises:

3 obtaining the user password cookie;
4 verifying that the user password cookie is valid; and
5 updating the user password cookie using the shared secret key.

1 7. The method of claim 6, wherein updating the user password cookie using the shared
2 secret key, comprises:

3 combining at least a user identification (ID) and password with a time stamp; and
4 encrypting the combined at least user ID, password and time stamp using the shared secret
5 key.

1 8. The method of claim 1, wherein the web server is part of a common authentication
2 ring having a shared secret key.

1 9. The method of claim 1, further comprising:
2 authenticating a second valid user requesting access to the web server.

1 10. The method of claim 9, wherein authenticating a second valid user requesting access
2 to the web server, comprises:
3 receiving a request to connect the second valid user to the web server; and
4 creating a second user password cookie using the shared secret key; and
5 transmitting the second user password cookie in response to the request to connect the second
6 valid user.

1 11. The method of claim 1, further comprising:
2 authenticating the valid user at a second web server, wherein the web server and the second
3 web server are part of a common authentication ring.

1 12. The method of claim 11, wherein authenticating the valid user at a second web server,
2 comprises:
3 receiving a request to connect the valid user to the second web server;

4 updating the user password cookie using the shared secret key; and
5 transmitting the user password cookie in response to the request to connect the valid user to
6 the second web server.

1 13. A computer-readable medium having stored therein a computer program for
2 providing distributed web server authentication of a valid user requesting access to a web server, said
3 program comprising:

4 receiving a request to connect a valid user to a web server;
5 creating a user password cookie using a shared secret key; and
6 transmitting the user password cookie in response to the request to connect.

1 14. The computer-readable medium of claim 13, wherein creating a user password cookie
2 using a shared secret key, comprises:

3 reading a user credential cookie;
4 requesting a user identification (ID) and password;
5 receiving the user ID and password; and
6 validating the valid user's identity.

1 15. The computer-readable medium of claim 14, wherein validating the valid user's
2 identity, comprises:

3 authenticating the user ID and password with the user credential cookie using a local
4 authenticating mechanism.

1 16. The computer-readable medium of claim 15, wherein the local authenticating
2 mechanism is an operating system.

1 17. The computer-readable medium of claim 14, wherein creating a user password cookie
2 using the shared secret key, further comprises:

3 combining at least the user ID and password with a time stamp; and

4 encrypting the combined at least user ID, password and time stamp using the shared secret
5 key.

1 18. The computer-readable medium of claim 13, wherein creating a user password cookie
2 using a shared secret key, comprises:

3 obtaining the user password cookie;
4 verifying that the user password cookie is valid; and
5 updating the password cookie using the shared secret key.

1 19. The computer-readable medium of claim 13, further comprising:
2 authenticating a second valid user requesting access to the web server.

1 20. The computer-readable medium of claim 19, wherein authenticating a second valid
2 user requesting access to the web server, comprises:
3 receiving a request to connect the second valid user to the web server; and
4 creating a second user password cookie using the shared secret key; and
5 transmitting the second user password cookie in response to the request to connect the second
6 valid user.

1 21. The computer-readable medium of claim 13, further comprising:
2 authenticating the valid user at a second web server, wherein the web server and the second
3 web server are part of a common authentication ring.

1 22. The computer-readable medium of claim 21, wherein authenticating the valid user at
2 a second web server, comprises:
3 receiving a request to connect the valid user to the second web server;
4 updating the user password cookie using the shared secret key; and
5 transmitting the user password cookie in response to the request to connect the valid user to
6 the second web server.

1 23. A computer-readable medium encoded with a data structure representing a password
2 cookie, said data structure comprising:
3 a user identification (ID);
4 a password; and
5 a time stamp associated with said user ID and password, wherein said password cookie is
6 encrypted using a shared secret key.

1 24. An apparatus for providing distributed web server authentication of a valid user
2 requesting access to a web server, said apparatus comprising:
3 a plurality of computer systems, wherein each of said plurality of computer systems is
4 coupled to at least one other of said plurality of computer systems, and wherein each of said plurality
5 of computer systems includes:
6 a processor unit;
7 a communications unit coupled to said processor unit;
8 a memory unit coupled to said processor unit; and
9 a computer program stored in the memory unit, said computer program, which, when
10 executed by the processor unit configures said computer system for:
11 receiving a request to connect the valid user to the computer system through
12 the communications unit;
13 creating a user password cookie using a shared secret key;
14 transmitting the user password cookie to the user.

1 25. A method of providing distributed web server authentication of a user, said method
2 comprising:
3 receiving a request to connect a user to a web server;
4 determining if the user is a valid user;
5 if the user is not valid, then,
6 denying access to the user;
7 if the user is valid, then,
8 if a valid user password cookie exists, then,
9 updating the user password cookie using a shared secret key;

10 if no valid user password cookie exists, then,
11 generating the user password cookie using the shared secret key;
12 transmitting the user password cookie to the user; and
13 connecting the web server to the user.

1 26. The method of claim 25, wherein determining if the user is a valid user, comprises:
2 reading a user credential cookie;
3 requesting a user identification (ID) and password;
4 receiving the user ID and password; and
5 validating the user's identity.

1 27. The method of claim 25, wherein determining if the user is a valid user, comprises:
2 obtaining the user password cookie;
3 verifying that the user password cookie is valid;
4 if the user password cookie is valid, then, the user is valid;
5 if the user password cookie is not valid, then, the user is not valid.

1 28. The method of claim 25, wherein the web server is part of a common authentication
2 ring having a shared secret key.

1 29. The method of claim 26, wherein generating the user password cookie using the
2 shared secret key, comprises:
3 combining at least the user ID and password with a time stamp; and
4 encrypting the combined at least user ID, password and time stamp using a shared secret key.

1 30. The method of claim 25, further comprising:
2 establishing a connection between the web server and a second user using a second
3 user password cookie and the shared secret key.

Add A3